ET99 多功能锁用户手册

V1.0 版

http://www.jansh.com.cn

坚石诚信科技有限公司

软件开发协议

坚石诚信科技有限公司（以下简称坚石）的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有订单都受本协议的制约。

1． 许可使用
   您可以将本软件合并、连接到您的计算机程序中，但其目的只是如使用手册中描述的那样保护您的程序或进行网络身份认证。您可以以备份为目的复制合理数量的拷贝。

2． 禁止使用
   除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、硬件和产品的其它部分。禁止对软件和产品的任何部分进行反向工程，禁止推导软件的源代码。禁止使用产品中的磁盘或光盘来传播、存储非本产品的原始内容的任何信息或由坚石提供的产品的任何升级。禁止将软件放在公共服务器上传播。

3． 有限担保
   坚石保证在自产品发给您之日起的 12 个月内，在正常的使用情况下，硬件和软件存储介质没有重大的工艺和材料上的缺陷。

4． 修理限度
   当根据本协议提出索赔时，坚石唯一的责任就是根据实际情况，免费进行替换或维修。坚石对被替换下来的任何产品部件都享有所有权。

   保修索赔单必须在担保期内写好，在发生故障 14 天内连同令人信服的证据交给坚石诚信科技公司。往返运费需由客户承担。

除了在本协议中保证的担保之外，坚石诚信科技公司不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负其它责任，包括它们的质量，性能和对某一特定目的的适应性。

5．责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，坚石诚信科技公司对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，坚石诚信科技公司对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使坚石诚信科技公司被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

6． 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2，3，4，5 将继续有效。

北京坚石诚信科技有限公司
地址：北京市海淀区学院路 40 号南一楼 2 层
邮编：100083
电话：010－62304411（总机）
传真：010－62304416
网址：http://www.jansh.com.cn

快速入门及注意事项

■ ET99多功能锁出厂设置为：

- PID（Product Identification）的初始值为8个字符“F”，即：“FFFFFFFF”。
- SO PIN (Super Officer Personal Identification Number)和USER PIN (User Personal Identification Number)的初始值为16个字符“F”，即：“FFFFFFFFFFFFFFFF”。
- SO PIN永远不锁死，USER PIN3次锁死，普通用户状态可以对数据存储区进行读写。
- 密钥存储区全为0xFF。
- 数据存储区全为0xFF。

■ 如果您需要使用ET99多功能锁进行开发或者测试请与我公司联系。开发需要的相关资料和软件接口请从我公司网站上下载。网址： http://www.jansh.com.cn

■ ET99多功能锁是USB接口的HID设备，在Win32的多种平台下都有系统自带的驱动支持，不需要安装额外的驱动程序。

■ ET99多功能锁具有64位全球唯一硬件序列号，及软件加密功能和身份认证功能于一身，适用于软件保护和安全系统身份认证。

■ ET99多功能锁的PID为8个（0－9，A－F）的字符，不区分大小写。SO PIN为16个（0－9，A－F）的字符，不区分大小写。USER PIN为16个（0－9，A－F）的字符，不区分大小写。

■ ET99多功能锁分为3级安全状态：匿名状态，普通用户状态（USER PIN验证通过），超级用户状态（SO PIN验证通过）。

- 超级用户状态下主要完成的工作：产生PID（用户打开多功能锁）、产生新的SO PIN、配置硬件设备、重新设置USER PIN，即解锁USER PIN。
- 普通用户状态下主要完成的工作：读写数据区中的数据、设置HMAC-MD5密钥、使用硬件中的HMAC-MD5算法进行计算。
- 另外，超级用户可以完成普通用户的所有操作。

■ ET99多功能锁的USER PIN和SO PIN最大重试次数可以设置为0－15次，当设置为0时，则表明USER PIN和SO PIN将永远不被锁死。如果开发商将SO PIN和USER PIN的最大重试次数设为1－15时，那么当使用者连续输入错误的次数达到了最大限制次数，则多功能锁锁死，这时即使输入正确的SO PIN和USER PIN，也不能进行相应的操作；如果在最大

限制次数内只要有一次输入正确，最大重试次数又恢复为开发商所设置的最大值。SO PIN和USER PIN的使用类似于生活中的银行卡。

■ 当USER PIN锁死时，可以使用SO PIN重置USER PIN为16个字符“F”。当SO PIN锁死时只能退换给我公司进行处理。

■ 当硬件设备配置成只读时，这时普通用户状态只能对数据存储区进行读操作，不能进行写操作，也不能设置HMAC-MD5密钥。超级用户状态可以进行写操作和设置HMAC-MD5密钥

■ ET99多功能锁提供1000字节的数据存储区域，必须经过USER PIN权限验证或者SO PIN权限验证后才可以进行读写操作。开发商也可以将该空间设置为只读，这时经过USER PIN权限验证后只可读取，不能写入；SO PIN验证后可读，可写。在使用读写接口进行读写操作时每次只能60个字节，多于60字节请分块操作。

■ ET99多功能锁提供密钥存储区域，开发商可以设置8个32字节的HMAC-MD5密钥。该密钥用于计算，只能被改写，无法读取。

■ 最终用户在使用ET99进行网上身份认证或者使用加密后的应用软件时，特别是在进行身份认证时需要输入ET99的USER PIN。由于ET99 的USER PIN为16个字符，用户输入不方便，这时开发商应先对USER PIN进行处理。可以将用户自己设定的USER PIN（如：superkey）通过调用我们接口库提供的MD5_HMAC接口或者自行设计相应的转换算法，将最终用户的输入转换成16个 （0－9，A－F）的字符。在使用MD5_HMAC接口时，其结果为16个字节，这时可以截取其中的8个字节，每个字节以2个字符（0－9，A－F）表示，这样再作为ET99的USER PIN，以供验证调用的接口使用。

■ ET99多功能锁提供外壳加密工具，通过此工具，您不需要编写一句代码，只需用鼠标作一些简单的选择操作，您便可以将 EXE、DLL、ARX 等 Win32 PE 结构的文件进行加密。

目　　录

第一章 简 介

1.1 关于 ET99 多功能锁

ET99 多功能锁是一款可以支持软件保护应用和身份认证应用的多功能，免驱动的 USB 设备。

对于受保护的软件，通过它，可以保护该软件不被非法复制和非授权访问或使用。当使用多功能锁加密保护您的软件后，启动所加密保护的程序时，此时若多功能锁不在或对某个应用模块的访问已超过预先设定的次数，程序会发出错误信息，从而终止，这就达到了加密保护软件的目的。ET99 多功能锁提供 API 接口调用和外壳加密等多种加密方式。

ET99 多功能锁还可以应用在各种安全系统身份认证领域，包括网站系统、OA 办公系统、信息查询系统等。通过 ET99 多功能锁的使用替换掉传统的用户名和密码，保证了系统的登录安全。

本手册会逐一论述 ET99 多功能锁的使用方法。

1.2 ET99 多功能锁实现软件保护的原理

通过在程序执行过程中对多功能锁的访问，进行读写等操作，使程序带有对多功能锁的硬件依赖性。利用多功能锁硬件专用芯片的不可复制性，使软件也具有不可复制性，从而实现软件保护的目的。开发商还可以使用外壳加密工具，不需要编写程序就可以对应用软件进行加密。建议加密过程采用API调用和外壳加密相结合，增加软件的加密的强度。

1.3 ET99 多功能锁实现身份认证原理

采用冲击响应的认证方法，登录时在服务器端和客户端同时进行计算，客户端计算前要先验证USER PIN，通过后在硬件中使用HMAC-MD5密钥进行计算，服务器端在服务器上使用软件进行计算，比较计算结果。

1.4 ET99 多功能锁的优点

- **兼容性好**

ET99多功能锁不仅对打印机、扫描仪等设备具有高度的透明性，特别是多个相同的ET99多功能锁也可以使用USB HUB并联在一起使用，相互之间不会干扰。

- **速度快**

对于使用ET99多功能锁加密后的软件，其运行速度同加密前区别不大，ET99多功能锁能够在很短的时间内处理完毕，保证用户程序的顺畅运行。

- **使用简便**

ET99多功能锁在API函数调用上从用户角度出发，最大限度简化使用接口。用户能够在很短的时间内掌握ET99多功能锁的使用方法，节约开发上所投入的时间。

- **高加密强度和身份认证相结合**

ET99多功能锁是全新设计的高强度多功能锁,有完整的用户管理。

（1）用户必须在超级用户状态下（SO PIN验证通过)，通过自己设定的不超过51字节的种子生成PID，以后打开和关闭多功能锁都需要通过PID来完成。PID的生成算法是在多功能锁内部完成的，而且是不可逆的，也就是说，只有生成者才知道什么样的种子能生成什么样的PID，别的人即使知道PID，同时也能够调用这个计算过程，但因为不知道种子是什么，是无法生成和您相同的PID的硬件，保证了用户的多功能锁的独特性。

（2）用户在对多功能锁中的数据进行读写操作时需要进行USER PIN验证，又增加了一层对软件的保护性。

（3）用户可以在配置设备时设为只读，那么多功能锁中的数据只可以读取，而不能被更改，密钥也不能被修改，从而保证了锁内数据不被篡改。

（4）使用多功能锁硬件中的HMAC-MD5算法进行冲击响应身份认证。HMAC-MD5密钥存在多功能锁中，该密钥只用于计算，任何人获取不到密钥的内容，保证密钥的安全性。

（5）提供了安全方便的外壳加密工具，使加密工作非常简单。

- **系统支持**

ET99多功能锁采用无驱设计，使用方便，兼容性好，支持多种操作系统台：Windows98（第二版）、Windows2000、WindowsXP、Windows2003等。

- **软件接口丰富**

ET99多功能锁提供3种接口：标准DLL动态链接库，全功能组件和安全组件。多种语言的调用示例：C#、ASP、DELPHI、VFP、VB、VC、JAVA、PB等。

第二章　ET99 多功能锁的硬件特性

2.1 ET99 多功能锁的内部构造

ET99多功能锁的核心是带USB接口的专用CPU。另外多功能锁CPU内部还有一片存储器芯片，存储的数据掉电后不会丢失。我们把它划分成数据存储区（1000字节）和密钥存储区（8个32字节密钥）。开发者可以将软件的一些重要信息(如序列号等)保存在多功能锁中的数据存储区中，或者将进行HMAC-MD5密钥写在多功能锁中的密钥存储区中。需要注意的是，存储区可写10万次，读的次数不受限制。10万次是个很大的数，一般完全可以满足绝大多数开发商的要求，只要不当成内存单元来使用就好。

2.2 ET99 多功能锁的硬件接口

ET99多功能锁支持 USB 1.1 标准，通过 USB HUB 进行扩展，并且在每个 USB 多功能锁上面有附加的信号灯，开发者可以通过信号灯来判定一些常见的问题（正常状态在插入 USB 多功能锁以后信号灯常亮，如果信号一闪一闪表示系统加载错误等）。另外ET99多功能锁提供了LED灯的控制接口，开发商可以自己编程控制LED灯的亮与灭。

2.3 ET99 多功能锁的安装问题

ET99多功能锁采用无驱设计，在win98二版以上的操作系统平台上不需要安装驱动程序。上层应用只需要调用DLL动态链接库提供的接口就可以对硬件进行各种操作。即插即用的，可随时插拔。但需要注意的是在比较干燥的环境下，主机和人体间可能存在很高的电压差(几百到几千伏)，若带电插拔，也可能会造成锁中芯片的过压损坏。USB 多功能锁虽然是即插即用，但如果在程序正在访问的过程中拔出多功能锁，也可能会导致系统的不稳定。

因为仅通过动态库来访问多功能锁，开发商可以将动态库打到自己的安装包中，或者通过IE插件的方式通过网页在线安装。

第三章　ET99 多功能锁的开发包

ET99多功能锁的开发包提供了开发商开发需要的工具和软件接口。开发商可以从我公司网站（http://www.jansh.com.cn）上下载相关资料。

- **ET99开发说明文档**

（1）ET99多功能锁用户手册.pdf：如何使用ET99多功能锁
（2）ET99多功能锁API接口.pdf：API接口说明
（3）全功能ActiveX控件参考手册.pdf：全功能ActiveX控件说明，适用于VB，Delphi，C#等
（4）安全ActiveX控件参考手册.pdf：安全ActiveX控件说明，适用于网页调用

- **开发头文件**

FT_ET99_API.h：开发头文件

- **动态链接库**

（1）FT_ET99_API.dll：标准DLL动态库
（2）FT_ET99_API.lib：动态Lib库
（3）ET99_MOD.dll：全功能ActiveX控件，其是建立在FT_ET99_API.dll基础上的。
（4）ET99_FULL.dll：安全ActiveX控件，其是建立在FT_ET99_API.dll基础上的
（5）JET99AI20.dll：JAVA的JNI接口DLL动态库
在使用ActiveX组件时，请将FT_ET99_API.dll，ET99_MOD.dll和ET99_FULL.dll拷贝到一起，并在命令行使用regsvr32命令进行注册，见5.2节。C#示例是使用的ET99_MOD.dll组件，网页中使用的是ET99_FULL.dll组件。

- **版权信息**

License.rtf：版权信息文件

- **示例程序**

包括VC、VB、Delphi、C#、ASP、JAVA、PB、FoxPro等示例代码

- **ET99多功能锁应用工具**

在运行各工具之前，请从lib目录下拷贝FT_ET99_API.dll文件到系统目录或当前目录。
(1)ET99Edit.exe－编辑器工具,实现了FT_ET99_API的全部接口。源代码参见ET99Edit源代码。
（2）SetSoPin.exe－设置新的SO PIN工具。源代码参见SetSoPin源代码。
（3）SetTokenPid.exe－设置PID工具，设置完PID后，用户可以正常使用ET99多功能锁。源代码参见SetTokenPid源代码。
（4）SetupToken.exe－配置硬件工具，设置SO PIN和USER PIN的重试次数，数据存储区的读写属性。源代码参见SetupToken源代码。
（5）ET99Env.exe－外壳加密工具。使用该工具对软件进行外壳加密。该工具运行时需要RyXShell_ET99.dll文件。源代码参见ET99Env源代码。

第四章　ET99 多功能锁工具使用

本章主要讲解Tools目录下的工具如何使用。出厂时硬件状态为：

● PID的初始值为8个字符“F”，即：“FFFFFFFF”。

● SO PIN和USER PIN的初始值为16个字符“F”，即：“FFFFFFFFFFFFFFFF”。

● SO PIN永远不锁死，USER PIN3次锁死，普通用户状态可以对数据存储区进行读写。

● 密钥存储区全为0xFF。

● 数据存储区全为0xFF。

用户可以使用下面介绍的工具更改为自己的值

另外，ET99多功能锁的PID为8个（0－9，A－F）的字符，不区分大小写。SO PIN为16个（0－9，A－F）的字符，不区分大小写。USER PIN为16个（0－9，A－F）的字符，不区分大小写。

4.1 SetSoPin 工具

该工具为设置新的SO PIN的工具，设置完成后，多功能锁的SO PIN更改为根据输入的不超过51个字节的种子而产生的新SO PIN。该示例源代码参见SetSoPin源代码。请开发商一定要记住SO PIN，一些操作只有经过SO PIN验证后才可以进行。如：

（1）产生PID（用户打开多功能锁）。

（2）产生新的SO PIN。

（3）配置硬件设备。

（4）重新设置USER PIN，即解锁USER PIN。

运行SetSoPin工具后，界面显示如下：

SetSOPIN

硬件PID: ffffffff

超级用户PIN码: ****************

种子: 123456

新的超级用户PIN码: FFC5EB786A2F0D73

设 置　　退 出

图4—1

- 硬件PID：输入PID，出厂为8个字符“F”，即：“FFFFFFFF”
- 超级用户PIN码：旧的SO PIN，出厂为16个字符“F”，即：“FFFFFFFFFFFFFFFF”
- 种子：产生新的SO PIN的种子，不要超过51字节

填写完成后点击设置按钮，弹出设置成功对话框。这时多功能锁的SO PIN为“新的超级用户PIN码”后面显示的16个字符，请开发商保存好。



图4—2

4.2 SetTokenPid 工具

PID为8个（0—9，A—F）的字符，不区分大小写，是打开锁时所必须的，打开锁时输入的PID与硬件的PID必须相同，否则是不能打开多功能锁的。PID出厂为8个字符“F”。开发商可以使用SetTokenPid工具进行更改，新的PID是根据用户输入的不超过51字节的

种子来产生的，这个过程是单向的，因此只要种子够复杂且保密，那么其他人是无法制作一个与该开发商PID相同的硬件，从而保证了多功能锁使用的安全性。设置PID时需要先进行SO PIN的验证。该示例源代码参见 SetTokenPid源代码。运行SetTokenPid工具后，界面显示如下：

图4－3

- 硬件PID：多功能锁当前的PID
- 超级用户PIN：多功能锁当前的SO PIN
- 种子：产生新PID的不超过51个字节的种子

填写完成后点击设置按钮，弹出成功的对话框。这时多功能锁的PID为“新的PID”后面显示的8个字符，以后打开多功能锁时需要输入这个新的PID，请开发商保留好。设置完PID后，多功能锁就可以正常使用了。



图4－4

4.3 ChangeUserPin 工具

该工具为更改USER PIN的工具，用户需要先输入ET99的硬件PID、旧的USER PIN和新的USER PIN，设置完成后，多功能锁的USER PIN更改为用户新输入的USER PIN。该示例源代码参见ChangeUserPin源代码。USER PIN的作用是：

（1）通过USER PIN的验证后，可以读取存储区中的数据。当存储区设置为可写时，可以写入数据。

（2）通过USER PIN验证后，可以设置HAMC_MD5密钥。

（3）通过USER PIN验证后，使用硬件的HAMC_MD5算法进行计算。

运行ChangeUserPin工具后，界面显示如下：



图4—5

- 硬件PID：输入ET99的硬件PID。
- 旧的用户PIN：输入ET99的旧的USER PIN，出厂为16个字符“F”，即：“FFFFFFFFFFFFFFFF”。
- 新的用户PIN：输入用户设定的新的USER PIN，注意USER PIN为16个（0—9，A—F）字符。
- 确认新的PIN：再次确认输入用户新的PIN。要与“新的用户PIN”中的一致。

填写完成后，点击修改按钮，弹出改变USER PIN成功对话框，这时ET99的USER PIN为用户新设置的USER PIN。



图4－6

4.4 SetupToken 工具

该工具主要设置SO PIN和USER PIN的使用次数，以及读写属性。该示例源代码参见SetupToken源代码。出厂设置为：SO PIN永远不锁死，USER PIN3次锁死，普通用户状态（USER PIN验证通过）可以对数据存储区进行读写。

开发商可以使用该工具进行设置。当SO PIN和USER PIN的最大重试次数设为0时，即SO PIN和USER PIN为永远不锁死，使用者可以一直反复试验SO PIN或者USER PIN，这时会有安全隐患。

如果开发商将SO PIN和USER PIN的最大重试次数设为1－15时，那么当使用者连续输入错误的次数达到了最大限制次数，则多功能锁锁死，这时即使输入正确的SO PIN和USER PIN，也不能进行相应的操作；如果在最大限制次数内只要有一次输入正确，最大重试次数又恢复为开发商所设置的最大值。SO PIN和USER PIN的使用类似于生活中的银行卡。

当USER PIN锁死时，可以使用SO PIN重置USER PIN为16个字符“F”。当SO PIN锁死时只能退换给我公司进行处理。

读写属性分为：

bUserReadOnly	数值	意义
ET_USER_WRITE_READ	0	可读写
ET_USER_READ_ONLY	1	只读

当设置为可读写时，使用者经过USER PIN验证后可以对数据存储区（1000字节）中的数据进行读写操作；可以设置密钥存储区（8个32字节）中的密钥。当设置为只读时，使用者经过USER PIN验证后只能对数据存储区中的数据进行读取操作，不能改写数据存储区中的数据，也不能设置密钥存储区中的密钥。

运行SetupToken工具后界面如下：

SetupToken

硬件PID: FFC5EB78

超级用户PIN: ****************

超级用户PIN码重试次数: 15

普通用户PIN码重试次数: 15

只读标志: 0

设　置　　退　出

图4—7

- 硬件PID：多功能锁当前的PID
- 超级用户PIN：多功能锁当前的SO PIN
- 超级用户PIN码重试次数：SO PIN最大重试次数
- 普通用户PIN码重试次数：USER PIN最大重试次数
- 只读标志：读写属性设置。0—可读写，1—只读

填写完成后按设置按钮，弹出设置成功对话框。



图4—8

4.5 ET99Edit 工具

ET99Edit工具实现了FT_ET99_API.dll全部的接口，其源代码参见ET99Edit源代码。

4.5.1 打开和关闭多功能锁

运行ET99Edit工具后，按“F”键，先进行查找多功能锁操作，这时输入多功能锁的PID，如下图：

```
Main menu:
------------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n           D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]       Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset           Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:f
Input PID <8>: ffc5eb78
Success!
Find 1 ET99.
```

图4—9

然后按“T”键，打开多功能锁，见下图：

```
Main menu:
------------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n           D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]       Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset           Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:t
Please input PID <8>: FFC5EB78
Success!
```

图4—10

按“C”键，关闭多功能锁。按“X”键则退出ET99Edit工具程序，见下图：

```
Main menu:
------------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:c

Close device:Success!
```

图4—11

4.5.2 验证 USER PIN，SO PIN 和重置安全状态

在打开多功能锁后，按“P”键，则验证USER PIN，这时可以进行普通用户权限的各种操作，见下图：

```
Main menu:
------------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:p
Input PIN <16>:ffffffffffffffff
Success!
```

图4—12

按“S”键进行SO PIN的操作，见下图：

```
Main menu:
------------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:s
Input SO PIN <16>:FFC5EB786A2F0D73
Success!
```

图4—13

按“R”键后，重置安全状态，即这时的硬件状态为匿名状态，见下图：

```
Main menu:
--------------------------------------------------------------
  [F]ind       Open[T]oken    LED[O]n          D[A]taMenu
  GetS[N]      GenP[I]D       GenRando[M]      Cr[Y]ptMenu
  User[P]IN    [S]OPIN        [R]eset          Set[U]pMenu
  LE[D]Off     [C]lose        E[X]it

Input selection:r
Reset token:Success!
```

图4—14

4.5.3 控制指示灯

在经过USER PIN验证或者SO PIN验证后，可以控制硬件指示灯的开关。按“O”键打开指示灯，按“D”键关闭指示灯。见下图：

```
Main menu:
--------------------------------------------------------------
  [F]ind       Open[T]oken    LED[O]n          D[A]taMenu
  GetS[N]      GenP[I]D       GenRando[M]      Cr[Y]ptMenu
  User[P]IN    [S]OPIN        [R]eset          Set[U]pMenu
  LE[D]Off     [C]lose        E[X]it

Input selection:o

Turn LED on:Success!


Main menu:
--------------------------------------------------------------
  [F]ind       Open[T]oken    LED[O]n          D[A]taMenu
  GetS[N]      GenP[I]D       GenRando[M]      Cr[Y]ptMenu
  User[P]IN    [S]OPIN        [R]eset          Set[U]pMenu
  LE[D]Off     [C]lose        E[X]it

Input selection:d

Turn LED off:Success!
```

图4—15

4.5.4 得到多功能锁的硬件 ID 和取随机数

在打开多功能锁后按“N”键可以得到硬件序列号，见下图：

```
Main menu:
--------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:n
Success!
The SN is :
31 32 33 34 35 36 37 38                                  12345678
```

图4—16

在经过USER PIN验证或者SO PIN验证后，可以取得随机数，见下图：

```
Main menu:
--------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:m
Generate random
Success!
DD 14 2B B7 8F 9D 7A 1F - 27 D8 64 9A 09 C3 20 7C     ..+...z.'.d... ¦
```

图4—17

4.5.5 产生 PID

在打开多功能锁，并验证SO PIN后，按“I”键产生PID，该功能与SetTokenPid工具的功能是一样的。见下图：

```
Main menu:
------------------------------------------------------------
  [F]ind        Open[T]oken     LED[O]n          D[A]taMenu
  GetS[N]       GenP[I]D        GenRando[M]      Cr[Y]ptMenu
  User[P]IN     [S]OPIN         [R]eset          Set[U]pMenu
  LE[D]Off      [C]lose         E[X]it

Input selection:i
Please input seed (1-51): 123456
Success!
The new PID is : FFC5EB78
```

图4－18

4.5.6 读写数据和设置密钥

在打开多功能锁后，并经过USER PIN或者SO PIN验证后，按“A”键进入数据操作菜单，见下图：

```
Data Menu:
------------------------------------------------------------
  [R]ead    [W]rite    Set[K]ey    E[X]it
```

图4－19

按“W”键进行写操作，先输入要写入的数据在数据存储区中的偏移位置，再输入要写入的数据，注意：在进行写操作时每次只能60个字节，多于60字节请分块操作。见下图：

```
Data Menu:
------------------------------------------------------------
  [R]ead    [W]rite    Set[K]ey    E[X]it

Input selection:w
Input offset to begin write <0-999>:0
Input data to write <0-60>:hello

 =>> 5 bytes to write.
68 65 6C 6C 6F                                         hello

Success!

 =>> 5 bytes written successfully!
```

图4－20

按“R”键进行读操作，先输入要读取的数据在数据存储区中的偏移位置，再输入要读取数据的长度。注意：在进行读操作时每次只能60个字节，多于60字节请分块操作。见下图：

```
Data Menu:
--------------------------------------------------------------
  [R]ead    [W]rite    Set[K]ey    E[X]it

Input selection:r
Input offset to begin read <0-999>:0
Input number of byte to read <0-60>:5
Success!

 =>> 5 (0x5) bytes read.
68 65 6C 6C 6F                                          hello
```

图4—21

按“K”键进行设置HMAC-MD5密钥的操作，先输入密钥的索引号，再输入32字节的密钥值，见下图：

```
Data Menu:
--------------------------------------------------------------
  [R]ead    [W]rite    Set[K]ey    E[X]it

Input selection:k
Input Key's index <1-8>:1
Input Key(32):1234567890
Success!
```

图4—22

4.5.7 进行软件和硬件 HMAC-MD5 运算

打开多功能锁后，并经过USER PIN或者SO PIN验证后，按“Y”键，进入加密计算菜单，见下图：

```
Input selection:y


Crypt Menu:
----------------------------------------------------------------------

  [M]akeHMACKey     [H]MAC      E[X]it
```

图4－23

按“M”键进行HMAC-MD5密钥设置，先输入密钥索引号，然后输入密钥值，这时接口会将输入的值进行计算产生32字节的密钥文件，写入索引号指定的密钥中，见下图：

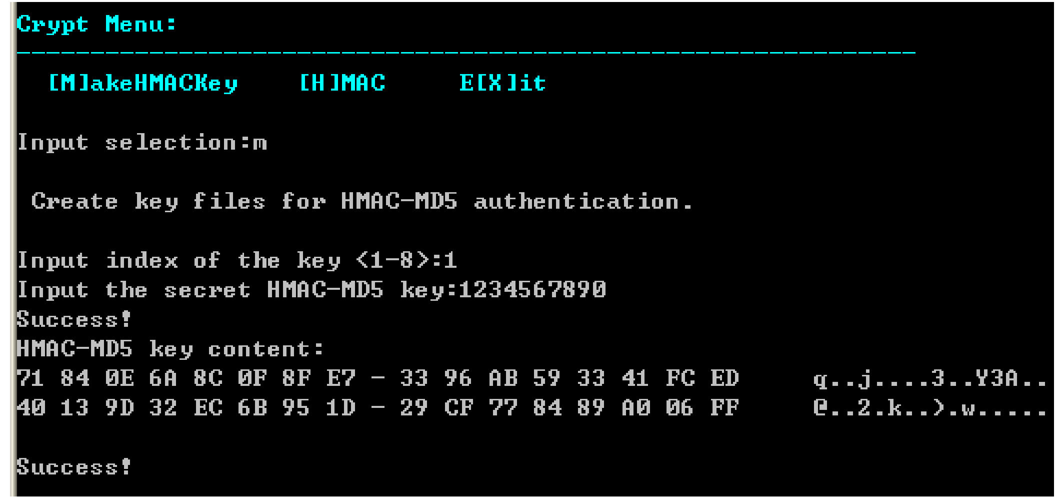


图4－24

按“H”键进行验证，这时先输入密钥索引号，然后输入随机数（不要超过51字节），这时在硬件中利用随机数和该索引号的密钥文件进行计算，得到计算结果。然后再输入密钥进行验证，密钥即上一步（按“M”键）产生32字节密钥文件的输入，这时接口使用软件进行计算，如果密钥一致则计算结果相同，见下图：

```
Crypt Menu:
------------------------------------------------------------
  [M]akeHMACKey     [H]MAC      E[X]it

Input selection:h

Using key for HMAC-MD5 authentication

Input index of the key (1-8):1
Input random data for HMAC-MD5 authentication(MAX 51 bytes):111111
Success!
1E 36 9C 42 03 4E 4B E5 - 8B 36 16 50 36 C3 37 48     .6.B.NK..6.P6.7H



Pleas input the secret HMAC-MD5 key to verify:1234567890
Success!
Software HMAC-MD5 compute result:
1E 36 9C 42 03 4E 4B E5 - 8B 36 16 50 36 C3 37 48     .6.B.NK..6.P6.7H

Verify successfully!
```

图4—25

上面的过程实际上就是冲击响应的过程，硬件中的计算为客户端的计算，软件计算为服务器端的计算，比较计算的结果，来判断登录用户的合法性。由于密钥在硬件中，没有人可以得到其内容，而进行计算前还需要进行USER PIN验证，因此保证了登录的安全性。

4.5.8 更改 SO PIN 和 USER PIN，解锁 USER PIN

打开多功能锁后，按“U”键进入设置菜单，见下图：

```
Input selection:u


Setup menu:
------------------------------------------------------------
  User[P]IN          Gen[S]OPIN          [R]esetUserPIN
  Setup[T]oken       E[X]it
```

图4—26

按“P”键可以对USER PIN进行更改，先输入旧的USER PIN，再输入新的USER PIN见下图：

```
Setup menu:
--------------------------------------------------------------
  User[P]IN           Gen[S]OPIN           [R]esetUserPIN
  Setup[T]oken        E[X]it


Input selection:p

Change User PIN
Input old User PIN <16>:ffffffffffffffff
Input new User PIN <16>:1111111111111111
Success!
```

图4—27

按“S”键设置新的SO PIN，但要先验证SO PIN，其功能与SetSoPin工具一样，先输入产生新的SO PIN的种子，不超过51字节，见下图：

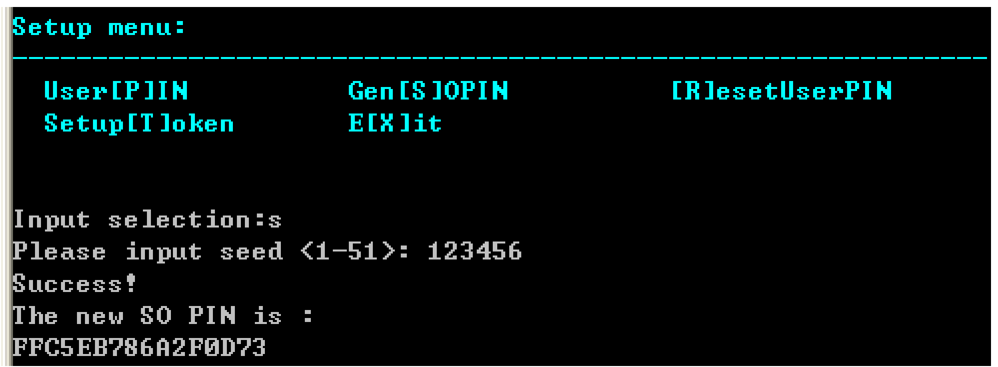


图4—28

按“R”键重新设置USER PIN为16个字符“F”，需要先输入SO PIN进行验证。在USER PIN锁死后，可以使用本功能进行解锁，见下图：

```
Setup menu:
------------------------------------------------------------
  User[P]IN            Gen[S]OPIN           [R]esetUserPIN
  Setup[T]oken         E[X]it


Input selection:r
Please input the SO PIN <16>: ffc5eb786a2f0d73
Success!
```

图4—29

按“T”键对硬件进行配置，需要先验证SO PIN，然后输入SO PIN的最大重试次数，USER PIN的重试次数，读写属性：0—可读写，1—只读。其功能与SetupToken工具功能一致，见下图：

```
Setup menu:
------------------------------------------------------------
  User[P]IN            Gen[S]OPIN           [R]esetUserPIN
  Setup[T]oken         E[X]it


Input selection:t
Please input SO PIN retry count <0-15>:15
Please input User PIN retry count <0-15>:15
Please input user read or write data zone flags <0 or 1>:0
Success!
```

图4—30

4.6 ET99Env 外壳加密工具

该工具运行时需要RyXShell_ET99.dll文件，源代码参见ET99Env源代码（相关下载\软件保护\外壳加密工具\ET99Env.rar）。开发商使用该工具对应用软件进行外壳加密，建议和API接口调用结合使用，增加软件的加密强度。该外壳工具只适用于标准的EXE、DLL、ARX 等 Win32 PE 结构的文件。运行ET99Env.exe后界面如下：

ET99Env v1.00.6.829
PID： FFC5EB78 USER PIN： **************
未加密的文件:
C:\WINDOWS\NOTEPAD.EXE
加密后的文件:
C:\WINDOWS\ET99_NOTEPAD.EXE
无锁警示窗口标题栏信息:
ET99加密锁
无锁警示窗口信息:
没有找到指定加密锁
进行后台定时检测 时间间隔(秒): 120 高级
硬件ID
加密成功 执行加密

图4－31

开发商填写ET99多功能锁的PID和USER PIN后，选择要加密的文件，点击执行加密按钮，进行外壳加密。

如果选择“进行后台定时检测”复选框，在时间间隔栏填写间隔时间（建议大于或者等于120秒），这时加密后的程序在经过设定的间隔时间时对ET99多功能锁硬件进行检查，以防止锁被拔下。点击高级按钮后出现对话框，来设置检测的方式，如下图：

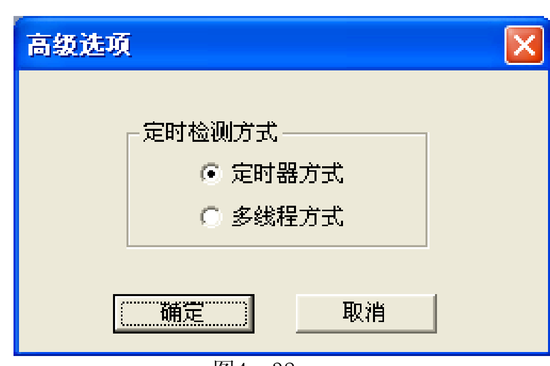


图4－32

定时器方式没有启用线程，是在应用程序的进程中检查硬件。多线程方式是启用线程来检查硬件。有窗口的应用程序可以使用上述二种方式，没有窗口的应用程序只能使用多线程方式。

如果选择“硬件ID”复选框，则加密后的程序与ET99多功能锁的硬件ID绑定，加密后的软件只能在正确的硬件ID的ET99多功能锁上运行。

在使用外壳工具加密后如出现错误，请按照下面的步骤检查：

（1） 有可能是输入的PID和USER PIN不正确造成的，这时可以使用ET99 Edit工具进行检测。请按照前面的4.5.1和4.5.2进行操作。

（2） 有可能是USER PIN锁死了，这时请按照前面的4.5.8进行解锁USER PIN操作。

（3） 有可能所加密的文件格式不支持，这时请使用系统中自带的NOTEPAD.EXE进行测试，该文件一般位于C:\WINDOWS\NOTEPAD.EXE。

第五章　ET99 多功能锁使用说明

5.1 使用 ET99 多功能锁加密软件

（1）ET99多功能锁提供1000字节的数据存储区，开发商可以使用该区域存储数据，有以下特点：

- 1000字节数据空间，可满足大部分应用软件需求。
- 需要通过PID打开多功能锁。
- 需要经过USER PIN或者SO PIN验证才可以进行操作。
- 可以设置为只读或者读写都可以。
- SO PIN和USER PIN可以设置为有最大次数限制，防止破解者反复尝试密码。
- 在使用读写接口进行读写操作时每次只能60个字节，多于60字节请分块操作。

（2）ET99密钥存储区可以存储8个32字节密钥，用于HMAC-MD5计算。实际上相当于种子码算法，通过输入（每次不超过51字节）进行计算，产生结果，将结果与应用软件中的数据进行加密处理，产生密文存储在多功能锁中。这样在应用软件使用时，必须通过该把多功能锁中的密钥计算产生的结果与密文进行反向解密处理产生明文，供软件使用。

（3）ET99多功能锁的外壳加密是保护您的软件最快捷的方法，使用外壳加密工具这种加密方案非常简单，对于没有源代码或没有很多时间编写代码加密的开发者是极为方便的。考虑到软件的发展趋势，我们的外壳加密工具目前仅对32位应用程序有效。目前支持的文件格式有 Win32 PE 格式 EXE、DLL，ARX 文件等。外壳工具的使用说明请参见第四章相应的说明。

开发包中有ET99Env外壳工具的VC源代码（相关下载\软件保护\外壳加密工具\ET99Env.rar），编译时需要将RyXShell_ET99.dll文件拷贝到系统目录中（如：C:\WINDOWS\system32）。

建议软件开发商灵活应用上述办法对应用软件进行加密。最好的方式是使用API函数接口完成加密工作后，再使用外壳工具再进行一次外壳加密，从而增加软件的加密强度。

5.2 使用 ET99 多功能锁进行身份认证

可以应用ET99多功能锁进行冲击响应身份认证，替换掉传统的用户名和密码方式，使登录更加安全。其原理如下图所示：

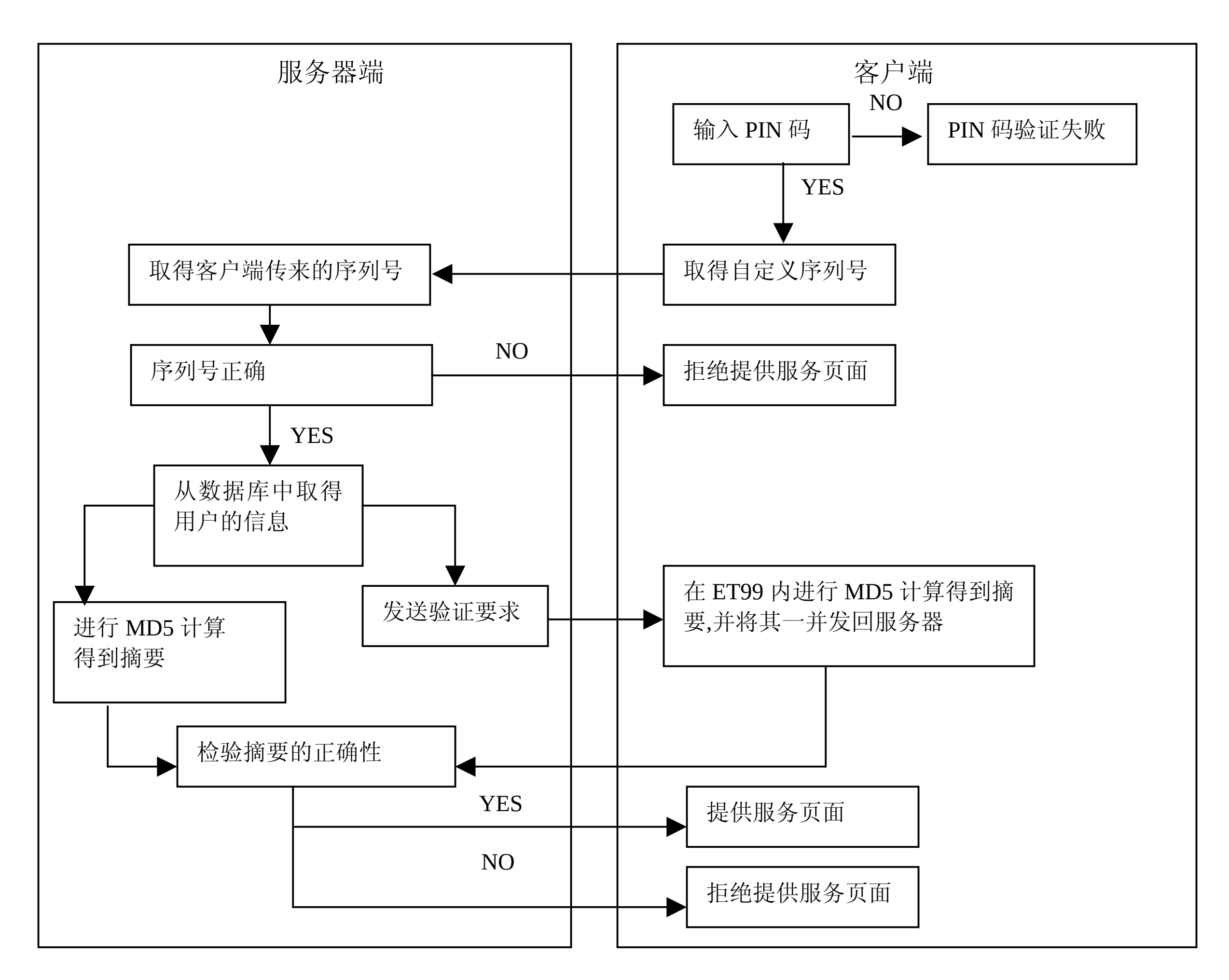


图5－1

在整个认证过程中，ET99采用冲击响应的认证方式。当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数并通过网络传输给客户端（此为冲击）。客户端将收到的随机数提供给ET99，由ET99使用该随机数与存储在ET99中的密钥进行HMAC-MD5运算并得到一个结果作为认证证据传给服务器（此为响应）。与此同时，服务器也使用该随机数与存储在服务器数据库中的该客

户密钥进行HMAC-MD5运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户。

具体可以参看ASP示例，其过程如下：

（1）使用ET99AspInit工具进行设置硬件计算所使用的HMAC-MD5密钥的工作，在使用该工具前需要将lib目录下的FT_ET99_API.dll文件拷贝到系统目录（system32目录）或当前目录。该工程的源代码参见ET99AspInit源代码（相关下载\身份认证\ET99 API示例，用在ASP示例中）。运行ET99AspInit.exe后界面如下图所示：

ET99 API Demo - VC

This demonstration program can create key in ET99 and save the "Key" into ET99 to used in ASP

This operation may take some time, please waiting...

PID: FFC5EB78

User PIN(16): ****************

Key: ******

Confirm Key: ******

OK　Cancel

图5—2

- PID：多功能锁当前的PID
- User PIN：多功能锁当前的USER PIN
- Key：用于产生进行HMAC-MD5计算的密钥，即认证密钥

填写完成后会弹出设置成功的对话框。如下图：



图5—3

正确设置HMAC-MD5密钥后，会在相同目录下产生一个user.txt文件，文件中记录着该把多功能锁的硬件ID和HMAC-MD5密钥值。如下图：

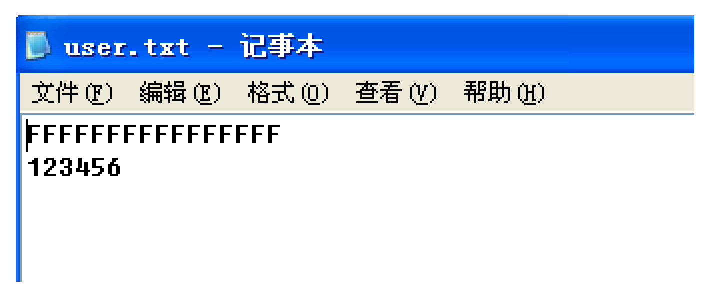


图5—4

（2）将Lib目录下的dll文件拷贝到系统的system32目录下，并在开始→运行→CMD中键入regsvr32 ET99_MOD.dll和regsvr32 ET99_FULL.dll，成功后会弹出注册组件成功的对话框。见下图：



图5—5



图5—6

（3）测试的机器上要安装了IIS服务器。在Asp文件夹单机右键，选择属性，然后选择Web 共享。见下图：

图5—7

（4）启动IE，浏览测试网页。输入多功能锁的PID和USER PIN。见下图：

ET99 Active Control
Demo Program for ASP

Welcome to ET99 Active Control demonstration program for ASP.

To logon, you must input Token Pid and your PIN.

Token Pid:	FFC5EB78
User PIN:	****************

Let me in　Re-input

Create by FeiTian, 2006-5-18
Copyright© 2006,Feitian Tech. Co. Ltd.

图5—8

按Let me in按钮后到验证页面，表示登录验证成功，见下图：

ET99 Active Control
Demo Program for ASP

Welcome to ET99 Active Control demonstration program for ASP.

Congratulation, FFFFFFFFFFFFFFFF ! You can get in now.

Create by FeiTian, 2006-5-18
Copyright© 2006,Feitian Tech. Co. Ltd.

图5—9

说明：本示例中服务器端使用的user.txt文件的方式，实际开发中应根据需要采用数据库。开发商可以将登录用户的用户名存储到多功能锁的数据存储区中，那么客户端在利用服务器产生的随机数进行完HMAC-MD5硬件计算后，将从硬件中读取的用户名，和客户端计算结果传递给服务器端。服务器利用用户名从数据库中取得该用户的密钥，利用随机数进行软件计算得到服务器端的结果，然后与客户端的结果进行比较，一致则表明用户身份合法。

在整个认证过程中网络上所传递的只有3种数据：用户名，随机数和计算结果，计算结果由随机数的不同而每次各不相同，这些数据被截取到也是没有意义的。同时ET99多功能锁是客户端的安全产品，具有以下特点：

- 登录用户必须先输入自己的USER PIN进行验证后才有权限完成计算。
- USER PIN有最大重试次数限制，连续输入错误会锁死。从而防止硬件丢失后，被不合法的用户反复重试。
- 存储在ET99多功能锁中的密钥不能被任何人获取。
- 用户登录时必须具备硬件和保护硬件的USER PIN双重因子时才能登录。有硬件，不知道USER PIN或者知道USER PIN，没有硬件，都是没有办法登录的。比传统的用户名和密码方式大大增加的登录用户的安全性。
- 保障了系统开发商的利益。使用硬件登录，不存在用户名密码共享的问题。

第六章　常见问题

本章能帮助您解决使用 ET99 多功能锁时碰到的一些常见问题。下面列出了一些您或您的客户可能遇到的一些问题，同时提出了决解方案。

6.1 一些问题的通常处理手段

■ 请留意我们的站点 http://www.jansh.com.cn 我们会经常更新这个站点。
■ 换另一台计算机进行测试，是否问题还出现。
■ 检查计算机是否受病毒感染（病毒可能阻止程序的正常运行）。

6.2 常见问题

1. 什么是USB接口，它有何优点？
答：USB接口的含义是通用串行总线，英文全称是Universal Serial Bus。是一种新的接口标准。可详见www.usb.org。优点是即插即用、支持热插拔、传输速度快、可通过扩展连接多达127个USB设备，不用担心USB多功能锁与打印机等外设的冲突。

2. 为什么我的USB多功能锁插上后显示未知设备？
答：一般有3种情况。（1）有干扰或是接触不良，重新插入或者更换计算机上的其它USB插口。（2）ET99多功能锁采用无驱设计，在win98二版以上的操作系统使用系统自带的驱动，不需要独立安装驱动。但在不完善的操作系统安装过程中会去掉系统驱动，用户需要在同版本的操作系统种将WINDOWS\Driver Cache\i386\driver.cab文件拷贝到不完善的操作系统的相应目录中。（3）请检查是否关闭了BIOS中的USB支持选项。

3. 硬件安装问题？
答：win98二版安装时需要win98的系统安装盘上的base6.cab包。Win2000/XP/2003以上操作系统不需要系统安装盘。如果在计算机上不能认到多功能锁，请使用USB鼠标或者USB键盘来检测计算机的系统是否支持标准HID设备。

4. 多功能锁如何进行软件更新？
答：如果您是我们的测试用户，您会定期收到我们寄给您的最新升级。如果不是，您可以去 http://www.jansh.com.cn上下载最新的开发包。

5. ET99多功能锁的PID是否安全？
答：非常安全。它是由一个长度不超过51个字节的字符串作为种子，多功能锁会根据这个种子生成 PID。这个生成算法是在多功能锁内部完成的，而且是不可逆的，也就是说，只有生成者才知道什么样的种子能生成什么样的PID，别的人即使知道PID，也能够调用这个计算过程，但因为不知道种子是什么，是无法生成您的PID的，从而无法生产出一个与您手中一致的多功能锁硬件。

6. ET99多功能锁的SO PIN和USER PIN是否安全？
答：非常安全。SO PIN和USER PIN可以设置成永远不锁死和锁死二种状态，开发商可以根据自己的情况灵活选择。当设置为锁死状态后，如果连续输入错误的次数超过了最大重试次数，则多功能锁锁死，这时输入正确的密码也不能进行相应的操作；在最大重试次数内只要有一次输入正确，则重试次数又恢复为最大重试次数。这种机制类似于银行卡，防止破坏者反复重试破解密码。当USER PIN锁死时，可以使用SO PIN重新设置USER PIN为16个字符“F”。但当SO PIN锁死时，只能退还给我们处理。

7. 开发时请注意ET99多功能锁的出厂设置。参看本手册开始的快速入门及注意事项。